МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

«ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ СИСТЕМ
УПРАВЛЕНИЯ И РАДИОЭЛЕКТРОНИКИ»
(ТУСУР)

УТВЕРЖДАЮ
Директор департамента образования
_____ П. Е. Троян
«___» _____ 20__ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Информационная безопасность и защита информации

Уровень образования: **высшее образование - бакалавриат**
Направление подготовки / специальность: **27.03.03 Системный анализ и управление**
Направленность (профиль) / специализация: **Системный анализ и управление в информационных технологиях**
Форма обучения: **очная**
Факультет: **ФВС, Факультет вычислительных систем**
Кафедра: **КСУП, Кафедра компьютерных систем в управлении и проектировании**
Курс: **4**
Семестр: **8**
Учебный план набора 2015 года

Распределение рабочего времени

№	Виды учебной деятельности	8 семестр	Всего	Единицы
1	Лекции	18	18	часов
2	Лабораторные работы	30	30	часов
3	Всего аудиторных занятий	48	48	часов
4	Самостоятельная работа	60	60	часов
5	Всего (без экзамена)	108	108	часов
6	Общая трудоемкость	108	108	часов
		3.0	3.0	З.Е.

Зачет: 8 семестр

Томск 2018

Согласована на портале № 33456

Рассмотрена и одобрена на заседании кафедры
протокол № 6 от «15» 5 2018 г.

ЛИСТ СОГЛАСОВАНИЯ

Рабочая программа дисциплины составлена с учетом требований федерального государственного образовательного стандарта высшего образования (ФГОС ВО) по направлению подготовки (специальности) 27.03.03 Системный анализ и управление, утвержденного 11.03.2015 года, рассмотрена и одобрена на заседании кафедры КИБЭВС «___» _____ 20__ года, протокол №_____.

Разработчик:
доцент каф. КИБЭВС _____ Е. Ю. Костюченко

Заведующий обеспечивающей каф.
КИБЭВС _____ А. А. Шелупанов

Рабочая программа дисциплины согласована с факультетом и выпускающей кафедрой:

Декан ФВС _____ Л. А. Козлова

Заведующий выпускающей каф.
КСУП _____ Ю. А. Шурыгин

Эксперты:

Доцент лаборатории безопасных биомедицинских технологий ЦТБ КИБЭВС _____ А. А. Конев

Доцент кафедры компьютерных систем в управлении и проектировании (КСУП) _____ Н. Ю. Хабибулина

Согласована на портале № 33456

1. Цели и задачи дисциплины

1.1. Цели дисциплины

Целью преподавания дисциплины является изучение комплекса проблем информационной безопасности предприятий и организаций различных типов и направлений деятельности, построения, функционирования и совершенствования совокупности правовых, организационных, технических и технологических процессов, обеспечивающих информационную безопасность и формирующих структуру системы защиты ценной и конфиденциальной информации в сфере охраны интеллектуальной собственности и сохранности информационных ресурсов.

1.2. Задачи дисциплины

- ознакомление студентов с теоретическими основами, основными понятиями и принципами обеспечения информационной безопасности
- обучение студентов работе с основными средствами защиты
-

2. Место дисциплины в структуре ОПОП

Дисциплина «Информационная безопасность и защита информации» (Б1.В.ОД.7) относится к блоку 1 (вариативная часть).

Предшествующими дисциплинами, формирующими начальные знания, являются: Информатика.

Последующими дисциплинами являются: Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты.

3. Требования к результатам освоения дисциплины

Процесс изучения дисциплины направлен на формирование следующих компетенций:

- ОПК-7 способностью к освоению новой техники, новых методов и новых технологий;
- ПК-4 способностью применять методы системного анализа, технологии синтеза и управления для решения прикладных проектно-конструкторских задач;

В результате изучения дисциплины обучающийся должен:

- **знать** базовые концепции и модели информационной безопасности; основы функционирования безопасности информационных систем задачи информационной безопасности; законодательство по обеспечению информационной безопасности стандарты в области информационной безопасности; методы и средства защиты информационной безопасности направления и методы ведения аналитической работы по выявлению угроз технические процедуры по действиям в нештатной ситуации; методологии оценки рисков и угроз информационной безопасности
- **уметь** выбирать (разрабатывать) стратегии защиты информационной безопасности различных информационных систем проводить аудит для отображения уровням соответствия стандартам области информационной безопасности для информационной системы в целом и для ее элементов оценивать и выбирать необходимые средства защиты осуществлять мониторинг состояния информационной безопасности объекта обеспечивать противодействие атакам на информационную систему выполнять (контролировать выполнение) требований инструкции по обеспечению информационной безопасности
- **владеть** навыками работы с программными и аппаратными средствами обеспечивающими защиту информации в компьютерных системах

4. Объем дисциплины и виды учебной работы

Общая трудоемкость дисциплины составляет 3.0 зачетных единицы и представлена в таблице 4.1.

Таблица 4.1 – Трудоемкость дисциплины

Виды учебной деятельности	Всего часов	Семестры
		8 семестр
Аудиторные занятия (всего)	48	48
Лекции	18	18

Согласована на портале № 33456

Лабораторные работы	30	30
Самостоятельная работа (всего)	60	60
Подготовка к контрольным работам	6	6
Выполнение индивидуальных заданий	6	6
Оформление отчетов по лабораторным работам	20	20
Проработка лекционного материала	24	24
Выполнение контрольных работ	4	4
Всего (без экзамена)	108	108
Общая трудоемкость, ч	108	108
Зачетные Единицы	3.0	3.0

5. Содержание дисциплины

5.1. Разделы дисциплины и виды занятий

Разделы дисциплины и виды занятий приведены в таблице 5.1.

Таблица 5.1 – Разделы дисциплины и виды занятий

Названия разделов дисциплины	Лек., ч	Лаб. раб., ч	Сам. раб., ч	Всего часов (без экзамена)	Формируемые компетенции
8 семестр					
1 Базовые понятия в сфере обеспечения информационной безопасности	2	0	2	4	ОПК-7, ПК-4
2 Комплексный подход к обеспечению информационной безопасности	2	0	2	4	ОПК-7, ПК-4
3 Организационно-правовое обеспечение, стандартизация, сертификация и лицензирование в области защиты информации	2	8	12	22	ПК-4
4 Методы оценки рисков и угроз информационной безопасности	2	2	14	18	ОПК-7, ПК-4
5 Программно-аппаратные, технические и криптографические средства защиты информации	2	16	8	26	ОПК-7, ПК-4
6 Основные принципы, направления и требования обеспечения информационной безопасности организации	2	0	8	10	ПК-4
7 Концепция и политика информационной безопасности	2	0	2	4	ПК-4
8 Реализации стратегии обеспечения информационной безопасности	2	4	8	14	ОПК-7, ПК-4
9 Менеджмент информационной безопасности	2	0	4	6	ОПК-7, ПК-4
Итого за семестр	18	30	60	108	
Итого	18	30	60	108	

Согласована на портале № 33456

5.2. Содержание разделов дисциплины (по лекциям)

Содержание разделов дисциплин (по лекциям) приведено в таблице 5.2.

Таблица 5.2 – Содержание разделов дисциплин (по лекциям)

Названия разделов	Содержание разделов дисциплины (по лекциям)	Трудоемкость, ч	Формируемые компетенции
8 семестр			
1 Базовые понятия в сфере обеспечения информационной безопасности	Информация. Конфиденциальность. Целостность. Доступность. Свойства информации. Угроза. Нарушитель.	2	ОПК-7
	Итого	2	
2 Комплексный подход к обеспечению информационной безопасности	Структура системы защиты информации.	2	ОПК-7
	Итого	2	
3 Организационно-правовое обеспечение, стандартизация, сертификация и лицензирование в области защиты информации	Основные нормативно правовые акты по защите информации. Стандартизация. Сертификация. Лицензирование.	2	ПК-4
	Итого	2	
4 Методы оценки рисков и угроз информационной безопасности	Оценка рисков. Информационные измерения. Нечеткая кластеризация. Идентификация и анализ рисков.	2	ОПК-7
	Итого	2	
5 Программно-аппаратные, технические и криптографические средства защиты информации	Управление доступом. Разграничение уровней доступа. Дискретное распределение доступа.Мандатное распределение доступа.	2	ПК-4
	Итого	2	
6 Основные принципы, направления и требования обеспечения информационной безопасности организации	Определение организационных требований защиты ИТ.	2	ПК-4
	Итого	2	
7 Концепция и политика информационной безопасности	Политика безопасности.	2	ПК-4
	Итого	2	
8 Реализации стратегии обеспечения информационной безопасности	Определение организационных целей и стратегий защиты ИТ. Идентификация и анализ угроз активам ИТ в пределах организации. Определение соответствующих защитных мер.	2	ПК-4
	Итого	2	

Согласована на портале № 33456

9 Менеджмент информационной безопасности	Контроль выполнения и функционирования защитных мер. Разработка и реализация программы осведомленности о защите. Обнаружение инцидентов и реагирование на них.	2	ПК-4
	Итого	2	
Итого за семестр		18	

5.3. Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами

Разделы дисциплины и междисциплинарные связи с обеспечивающими (предыдущими) и обеспечиваемыми (последующими) дисциплинами представлены в таблице 5.3.

Таблица 5.3 – Разделы дисциплины и междисциплинарные связи

Наименование дисциплин	№ разделов данной дисциплины, для которых необходимо изучение обеспечивающих и обеспечиваемых дисциплин								
	1	2	3	4	5	6	7	8	9
Предшествующие дисциплины									
1 Информатика	+	+	+	+	+	+	+	+	+
Последующие дисциплины									
1 Защита выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты	+	+	+	+	+	+	+	+	+

5.4. Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий представлено в таблице 5.4.

Таблица 5.4 – Соответствие компетенций, формируемых при изучении дисциплины, и видов занятий

Компетенции	Виды занятий			Формы контроля
	Лек.	Лаб. раб.	Сам. раб.	
ОПК-7	+	+	+	Отчет по индивидуальному заданию, Выполнение контрольной работы, Отчет по лабораторной работе, Зачет, Тест
ПК-4	+	+	+	Контрольная работа, Отчет по индивидуальному заданию, Выполнение контрольной работы, Отчет по лабораторной работе, Зачет, Тест

6. Интерактивные методы и формы организации обучения

Не предусмотрено РУП.

7. Лабораторные работы

Наименование лабораторных работ приведено в таблице 7.1.

Согласована на портале № 33456

Таблица 7.1 – Наименование лабораторных работ

Названия разделов	Наименование лабораторных работ	Трудоемкость, ч	Формируемые компетенции
8 семестр			
3 Организационно-правовое обеспечение, стандартизация, сертификация и лицензирование в области защиты информации	Защита персональных данных и коммерческой тайны	4	ПК-4
	Политика безопасности и инструкции для сотрудников предприятия	4	
	Итого	8	
4 Методы оценки рисков и угроз информационной безопасности	Оценка рисков информационной безопасности	2	ПК-4
	Итого	2	
5 Программно-аппаратные, технические и криптографические средства защиты информации	Защита компьютерной информации на уровне доступа в систему	4	ПК-4, ОПК-7
	Защита от атак по локальным и глобальным сетям	2	
	Защита от вредоносного ПО	2	
	Использование шифрования для защиты данных	4	
	Использование физических носителей и защитных систем на их основе	4	
	Итого	16	
8 Реализации стратегии обеспечения информационной безопасности	Разработка системы защиты предприятия	4	ОПК-7
	Итого	4	
Итого за семестр		30	

8. Практические занятия (семинары)

Не предусмотрено РУП.

9. Самостоятельная работа

Виды самостоятельной работы, трудоемкость и формируемые компетенции представлены в таблице 9.1.

Таблица 9.1 – Виды самостоятельной работы, трудоемкость и формируемые компетенции

Названия разделов	Виды самостоятельной работы	Трудоемкость, ч	Формируемые компетенции	Формы контроля
8 семестр				
1 Базовые понятия в сфере обеспечения информационной	Проработка лекционного материала	2	ПК-4	Зачет, Тест
	Итого	2		

Согласована на портале № 33456

безопасности				
2 Комплексный подход к обеспечению информационной безопасности	Проработка лекционного материала	2	ПК-4	Зачет, Тест
	Итого	2		
3 Организационно-правовое обеспечение, стандартизация, сертификация и лицензирование в области защиты информации	Проработка лекционного материала	4	ПК-4	Выполнение контрольной работы, Зачет, Отчет по лабораторной работе, Тест
	Оформление отчетов по лабораторным работам	4		
	Подготовка к контрольным работам	4		
	Итого	12		
4 Методы оценки рисков и угроз информационной безопасности	Проработка лекционного материала	2	ОПК-7	Зачет, Отчет по индивидуальному заданию, Отчет по лабораторной работе, Тест
	Оформление отчетов по лабораторным работам	8		
	Выполнение индивидуальных заданий	4		
	Итого	14		
5 Программно-аппаратные, технические и криптографические средства защиты информации	Проработка лекционного материала	4	ОПК-7	Зачет, Отчет по лабораторной работе, Тест
	Оформление отчетов по лабораторным работам	4		
	Итого	8		
6 Основные принципы, направления и требования обеспечения информационной безопасности организации	Выполнение контрольных работ	4	ПК-4	Выполнение контрольной работы, Зачет, Тест
	Проработка лекционного материала	4		
	Итого	8		
7 Концепция и политика информационной безопасности	Проработка лекционного материала	2	ПК-4	Зачет, Тест
	Итого	2		
8 Реализации стратегии обеспечения информационной безопасности	Проработка лекционного материала	2	ПК-4, ОПК-7	Зачет, Отчет по индивидуальному заданию, Отчет по лабораторной работе, Тест
	Оформление отчетов по лабораторным работам	4		
	Выполнение индивидуальных заданий	2		
	Итого	8		
9 Менеджмент информационной безопасности	Проработка лекционного материала	2	ОПК-7	Выполнение контрольной работы, Зачет, Тест
	Подготовка к контрольным работам	2		
	Итого	4		

Согласована на портале № 33456

Итого за семестр	60		
Итого	60		

10. Курсовая работа (проект)

Не предусмотрено РУП.

11. Рейтинговая система для оценки успеваемости обучающихся

11.1. Балльные оценки для элементов контроля

Таблица 11.1 – Балльные оценки для элементов контроля

Элементы учебной деятельности	Максимальный балл на 1-ую КТ с начала семестра	Максимальный балл за период между 1КТ и 2КТ	Максимальный балл за период между 2КТ и на конец семестра	Всего за семестр
8 семестр				
Выполнение контрольной работы	7	7	7	21
Зачет			15	15
Контрольная работа	5	5	5	15
Отчет по индивидуальному заданию	11		11	22
Отчет по лабораторной работе	5	5	5	15
Тест	4	4	4	12
Итого максимум за период	32	21	47	100
Нарастающим итогом	32	53	100	100

11.2. Пересчет баллов в оценки за контрольные точки

Пересчет баллов в оценки за контрольные точки представлен в таблице 11.2.

Таблица 11.2 – Пересчет баллов в оценки за контрольные точки

Баллы на дату контрольной точки	Оценка
≥ 90% от максимальной суммы баллов на дату КТ	5
От 70% до 89% от максимальной суммы баллов на дату КТ	4
От 60% до 69% от максимальной суммы баллов на дату КТ	3
< 60% от максимальной суммы баллов на дату КТ	2

11.3. Пересчет суммы баллов в традиционную и международную оценку

Пересчет суммы баллов в традиционную и международную оценку представлен в таблице 11.3.

Таблица 11.3 – Пересчет суммы баллов в традиционную и международную оценку

Оценка (ГОС)	Итоговая сумма баллов, учитывает успешно сданный экзамен	Оценка (ECTS)
5 (отлично) (зачтено)	90 - 100	A (отлично)
4 (хорошо) (зачтено)	85 - 89	B (очень хорошо)
	75 - 84	C (хорошо)
	70 - 74	D (удовлетворительно)

Согласована на портале № 33456

3 (удовлетворительно) (зачтено)	65 - 69	
	60 - 64	E (посредственно)
2 (неудовлетворительно) (не зачтено)	Ниже 60 баллов	F (неудовлетворительно)

12. Учебно-методическое и информационное обеспечение дисциплины

12.1. Основная литература

1. Основы защиты информации. Учебное пособие / Шелупанов А.А., Сопов М.А. и др., Издание пятое, перераб. и допол. Гриф СибРОУМО. – Томск: Изд-во «В-Спектр», 2011. – 244 с. ISBN 978-5-91191-214-7 [Электронный ресурс] - Режим доступа: http://kibevs.tusur.ru/sites/default/files/upload/manuals/shelupanov_ozi.pdf (дата обращения: 25.06.2018).

12.2. Дополнительная литература

1. Нормативно-правовые акты информационной безопасности. Учебное пособие / Шелупанов А.А., Сопов М.А. и др. В трех частях. Ч.1. Издание седьмое, перераб. и допол. – Гриф СибРОУМО Томск: В-Спектр, 2011. - 223с. ISBN 978-5-91191-227-9 [Электронный ресурс] - Режим доступа: http://kibevs.tusur.ru/sites/default/files/upload/manuals/sopov_poib/npa-ib-1ch.pdf (дата обращения: 25.06.2018).
2. Нормативно-правовые акты информационной безопасности. Учебное пособие / Шелупанов А.А., Сопов М.А. и др. В трех частях. Ч.2. Издание седьмое, перераб. и допол. – Гриф СибРОУМО Томск: В-Спектр, 2011. - 223с. ISBN 978-5-91191-227-9 [Электронный ресурс] - Режим доступа: http://kibevs.tusur.ru/sites/default/files/upload/manuals/sopov_poib/npa-ib-2ch.pdf (дата обращения: 25.06.2018).
3. Нормативно-правовые акты информационной безопасности. Учебное пособие / Шелупанов А.А., Сопов М.А. и др. В трех частях. Ч.3. Издание седьмое, перераб. и допол. – Гриф СибРОУМО Томск: В-Спектр, 2011. - 223с. ISBN 978-5-91191-227-9 [Электронный ресурс] - Режим доступа: http://kibevs.tusur.ru/sites/default/files/upload/manuals/sopov_poib/npa-ib-3ch.pdf (дата обращения: 25.06.2018).

12.3. Учебно-методические пособия

12.3.1. Обязательные учебно-методические пособия

1. «Методические указания к лабораторным работам по дисциплине «Информационная безопасность», / Конев А. А., Костюченко Е.Ю., Сопов М.А. 2011. – 39 с. [Электронный ресурс] - Режим доступа: http://kibevs.tusur.ru/sites/default/files/upload/manuals/sma/gf_isr/ib/metod_lab.pdf (дата обращения: 25.06.2018).
2. «Методические указания по самостоятельной и индивидуальной работе по дисциплине «Информационная безопасность»» / Сопов М.А., 2012г. – 2 с. [Электронный ресурс] - Режим доступа: http://keva.tusur.ru/sites/default/files/upload/manuals/sma/gf_isr/ib/metod_srs.pdf (дата обращения: 25.06.2018).

12.3.2. Учебно-методические пособия для лиц с ограниченными возможностями здоровья и инвалидов

Учебно-методические материалы для самостоятельной и аудиторной работы обучающихся из числа лиц с ограниченными возможностями здоровья и инвалидов предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации.

Для лиц с нарушениями зрения:

- в форме электронного документа;
- в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:

- в форме электронного документа;
- в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

- в форме электронного документа;

Согласована на портале № 33456

– в печатной форме.

12.4. Профессиональные базы данных и информационные справочные системы

1. https://lib.tusur.ru/
2. https://edu.tusur.ru/
3. Рекомендуется использовать информационные, справочные и нормативные базы данных https://lib.tusur.ru/ru/resursy/bazy-dannyh

13. Материально-техническое обеспечение дисциплины и требуемое программное обеспечение

13.1. Общие требования к материально-техническому и программному обеспечению дисциплины

13.1.1. Материально-техническое и программное обеспечение для лекционных занятий

Для проведения занятий лекционного типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации используется учебная аудитория с количеством посадочных мест не менее 22-24, оборудованная доской и стандартной учебной мебелью. Имеются демонстрационное оборудование и учебно-наглядные пособия, обеспечивающие тематические иллюстрации по лекционным разделам дисциплины.

13.1.2. Материально-техническое и программное обеспечение для лабораторных работ

Лаборатория алгоритмического обеспечения

учебная аудитория для проведения занятий лекционного типа, учебная аудитория для проведения занятий практического типа, учебная аудитория для проведения занятий лабораторного типа, помещение для проведения текущего контроля и промежуточной аттестации, помещение для самостоятельной работы

634034, Томская область, г. Томск, Вершинина улица, д. 74, 327 ауд.

Описание имеющегося оборудования:

- Интерактивная доска SMARTBOARD;
- ПЭВМ: SWS-1, SWS-2, SWS-3, SWS-4, SWS-5, SWS-6, SWS-7, SWS-8, SWS-9, SWS-10, SWS-11;
- Комплект специализированной учебной мебели;
- Рабочее место преподавателя.

Программное обеспечение:

– Windows XP Professional

13.1.3. Материально-техническое и программное обеспечение для самостоятельной работы

Для самостоятельной работы используются учебные аудитории (компьютерные классы), расположенные по адресам:

- 634050, Томская область, г. Томск, Ленина проспект, д. 40, 233 ауд.;
- 634045, Томская область, г. Томск, ул. Красноармейская, д. 146, 201 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 47, 126 ауд.;
- 634034, Томская область, г. Томск, Вершинина улица, д. 74, 207 ауд.

Состав оборудования:

- учебная мебель;
- компьютеры класса не ниже ПЭВМ INTEL Celeron D336 2.8ГГц. - 5 шт.;
- компьютеры подключены к сети «Интернет» и обеспечивают доступ в электронную информационно-образовательную среду университета.

Перечень программного обеспечения:

- Microsoft Windows;
- OpenOffice;
- Kaspersky Endpoint Security 10 для Windows;
- 7-Zip;

Согласована на портале № 33456

- Google Chrome.

13.2. Материально-техническое обеспечение дисциплины для лиц с ограниченными возможностями здоровья и инвалидов

Освоение дисциплины лицами с ограниченными возможностями здоровья и инвалидами осуществляется с использованием средств обучения общего и специального назначения.

При занятиях с обучающимися **с нарушениями слуха** предусмотрено использование звукоусиливающей аппаратуры, мультимедийных средств и других технических средств приема/передачи учебной информации в доступных формах, мобильной системы преподавания для обучающихся с инвалидностью, портативной индукционной системы. Учебная аудитория, в которой занимаются обучающиеся с нарушением слуха, оборудована компьютерной техникой, аудиотехникой, видеотехникой, электронной доской, мультимедийной системой.

При занятиях с обучающимися **с нарушениями зрениями** предусмотрено использование в лекционных и учебных аудиториях возможности просмотра удаленных объектов (например, текста на доске или слайда на экране) при помощи видеоувеличителей для комфортного просмотра.

При занятиях с обучающимися **с нарушениями опорно-двигательного аппарата** используются альтернативные устройства ввода информации и другие технические средства приема/передачи учебной информации в доступных формах, мобильной системы обучения для людей с инвалидностью.

14. Оценочные материалы и методические рекомендации по организации изучения дисциплины

14.1. Содержание оценочных материалов и методические рекомендации

Для оценки степени сформированности и уровня освоения закрепленных за дисциплиной компетенций используются оценочные материалы в составе:

14.1.1. Тестовые задания

1. Какая из нижеперечисленных задач, изложенных в Доктрине информационной безопасности Российской Федерации, не относится к задачам государственных органов в рамках деятельности по обеспечению информационной безопасности:

a) обеспечение защиты прав и законных интересов граждан и организаций в информационной сфере;

b) оценка состояния информационной безопасности, прогнозирование и обнаружение информационных угроз, определение приоритетных направлений их предотвращения и ликвидации последствий их проявления;

c) планирование и разработка мер по проведению киберразведовательных операций;

d) организация деятельности и координация взаимодействия сил обеспечения информационной безопасности, совершенствование их правового, организационного, оперативно-разыскного, разведывательного, контрразведывательного, научно-технического, информационно-аналитического, кадрового и экономического обеспечения;

2. В стандарте США "Критерии оценки гарантировано защищенных вычислительных систем в интересах министерства обороны США" в зависимости от конкретных значений, которым отвечают автоматизированные системы, они разделены на… a

) 5 классов;

b) 4 группы;

c) 3 множества;

d) 2 подгруппы.

3. Что из нижеперечисленного не относится к перечню сведений конфиденциального характера, утвержденного Президентом Российской Федерации?

a) Служебные сведения, доступ к которым ограничен органами государственной власти в соответствии с Гражданским кодексом Российской Федерации и федеральными законами (служебная тайна);

b) Защищаемые государством сведения в области его военной, внешнеполитической, эконо-

Согласована на портале № 33456

мической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации;

c) Сведения, связанные с профессиональной деятельностью, доступ к которым ограничен в соответствии с Конституцией Российской Федерации и федеральными законами (врачебная, нотариальная, адвокатская тайна, тайна переписки, телефонных переговоров, почтовых отправлений, телеграфных или иных сообщений и так далее);

4. Стандарт США «Критерии оценки гарантировано защищенных вычислительных систем в интересах министерства обороны США» называют …

a) «Желтой книгой»;

b) «Оранжевым документом»;

c) «Оранжевой книгой»;

d) «Красным списком».

5. Модель угроз безопасности информации не включает в себя:

a) Описание информационной системы и ее структурно-функциональных характеристик;

b) Описание угроз безопасности информации;

c) Описание возможностей нарушителей (модель нарушителя), возможных уязвимостей информационной системы;

d) Стадии (этапы работ) создания системы защиты информационной системы.

6. При макетировании и тестировании системы защиты информации информационной системы в том числе осуществляются:

a) Проверка работоспособности и совместимости выбранных средств защиты информации с информационными технологиями и техническими средствами;

b) Установка средств мониторинга сетевой инфраструктуры;

c) Разработка документов, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты информации в информационной системе в ходе ее эксплуатации;

d) Внедрение документов, регламентирующих организационные меры по защите информации;

7. Методический документ ФСТЭК России «Методика определения безопасности информации в информационных системах» применяется совместно с:

a) Базой данных уязвимостей, разработанной Федеральной службой безопасности Российской Федерации

b) Банком данных угроз безопасности информации, сформированным ФСТЭК России (ubi.fstec.ru);

c) Общедоступной базой данных компьютерных угроз;

d) Перечнем сведений конфиденциального характера.

8. Анализ уязвимостей информационной системы проводится в целях:

a) Оценки возможности преодоления нарушителем системы защиты информации информационной системы и предотвращения реализации угроз безопасности информации;

b) Оценки эффективности использования политик разграничения доступа;

c) Оптимизации производительности программно-аппаратных средств защиты информации;

d) Сегментации информационной системы.

9. Системный процесс получения объективных качественных и количественных оценок о текущем состоянии информационной безопасности компании в соответствии с определёнными критериями и показателями безопасности называется:

a) Аттестация;

b) Аудит;

c) Сертификация;

d) Пентест.

Согласована на портале № 33456

10. Что из нижеперечисленного не относится к международным методикам проведения тестирования на проникновение, ориентированных на моделирование атак, направленных на сетевую инфраструктуру организации:

a) Trusted Computer System Evaluation Criteria;

b) PCI DSS;

c) NIST SP800-115;

d) Open Source Security Testing Methodology Manual.

11. Абстрактное (формализованное или неформализованное) описание нарушителя правил разграничения доступа называется:

a) Характеристика нарушителя;

b) Модель нарушителя;

c) Сценарий нарушителя;

d) Модель источников угроз.

12. Какое из нижеперечисленных направлений не относится к аттестации объектов информатизации по требованиям безопасности информации:

a) Аттестация автоматизированных систем, средств связи, обработки и передачи информации;

b) Аттестация помещений, предназначенных для ведения конфиденциальных переговоров;

c) Аттестация рабочих мест с целью оценки условий труда;

d) Аттестация технических средств, установленных в выделенных помещениях и защищаемых помещениях.

13. Стратегия (метод) тестирования функционального поведения объекта (программы, системы) с точки зрения внешнего мира, при котором не используется знание о внутреннем устройстве тестируемого объекта

a) Тестировение черного ящика;

b) Тестирование белого ящика;

c) Тестирование красного ящика;

d) Тестирование неизвестного ящика.

14. Методика тестирования на проникновение называется:

a) Аудит;

b) Пентест;

c) Honeypot;

d) Metasploit.

15. Что из нижеперечисленного не относится к этапу анализа рисков информационной безопасности:

a) Построение модели нарушителя;

b) Идентификация ресурсов;

c) Идентификация бизнес-требований и требований законодательства, применимых к идентифицированным ресурсам;

d) Оценивание идентифицированных ресурсов с учетом выявленных бизнес требований и требований законодательства, а также последствий нарушения их конфиденциальности, целостности и доступности.

16. Какая угроза безопасности информации является преднамеренной ?

a) Ошибки персонала;

b) Сбой программного обеспечения;

c) Фальсификация, подделка документов;

d) Открытие электронного письма, содержащего вирус.

Согласована на портале № 33456

17. Территория вокруг помещений автоматизированной системы обработки данных, которая непрерывно контролируется персоналом или средствами автоматизированной системы обработки данных называется …

a) Неконтролируемой зоной
b) Зоной помещений автоматизированной системы
c) Зоной баз данных защищаемой системы
d) Зоной контролируемой территории.

18. Угроза диверсии относится к …

a) Субъективной преднамеренной причине нарушения целостности информации;
b) Субъективной непреднамеренной причине нарушения целостности информации;
c) Объективной непреднамеренной причине нарушения целостности информации;
d) Объективной преднамеренной причине нарушения целостности информации.

19. Перехват данных является угрозой:

a) Доступности;
b) Конфиденциальности;
c) Целостности;
d) Достоверности.

20. Продолжите тезис верно: Класс задач «Легендирование» по защите информации…

a) Не существует;
b) Потерял актуальность в связи с переходом на новые стандарты симметричных криптосистем;
c) Предполагает включение в состав элементов системы обработки информации дополнительных компонентов;
d) Объединяет задачи по обеспечению получения злоумышленником искаженного представления о характере и предназначении объекта.

21. Риск информационной безопасности это

a) Число уязвимостей в системе;
b) Отношение стоимости системы защиты к вероятности её «простоя»;
c) Сочетание вероятности угрозы информационной безопасности и последствий её наступления;
d) Оценка стоимости защитных средств.

22. Совокупность условий и факторов, определяющих потенциальную или реально существующую опасность нарушения конфиденциальности, целостности, доступности информации называется …

a) Угрозой безопасности;
b) Компьютерной безопасностью;
c) Анализом угроз;
d) Атакой на информационную систему.

23. Что из перечисленного происходит при использовании RAID-массивов?

a) Производится полное шифрование данных
b) Обеспечивается более высокий уровень защиты от вирусов
c) Повышается надёжность хранения данных
d) Увеличивается максимальная пропускная способность сети

24. Заключительным этапом построения системы защиты является …

a) Анализ уязвимых мест;
b) Планирование;

Согласована на портале № 33456

c) Обследование;
d) Сопровождение.

25. Что из перечисленного не используется в биометрической аутентификации?
a) Рисунок папиллярного узора;
b) Клавиатурный почерк;
c) Пластиковая карта с магнитной полосой;
d) Радужная оболочка глаза.

26. К какой подсистеме не предъявляются требования в Руководящем документе «Классификация автоматизированных систем и требований по защите информации»?
a) управления доступом;
b) регистрации и учета;
c) технической защиты информации;
d) обеспечения целостности.

27. Защита информации это:
a) Деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё;
b) Совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;
c) Процесс сбора, накопления, обработки, хранения, распределения и поиска информации;
d) Получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств.

28. Уровень безопасности С, согласно "Оранжевой книге", характеризуется:
a) Отсутствием управления доступом.
b) Произвольным управлением доступом;
c) Принудительным управлением доступом;
d) Верифицируемой безопасностью.

29. Свойство доступности достигается за счет применения мер, направленных на повыше
ние:
a) Аутентичности;
b) Непротиворечивости;
c) Отказоустойчивости;
d) Неотказуемости.

30. Каким термином называется защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативнорозыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации?
a) Конфиденциальная информация;
b) Секретная информация;
c) Военная тайна;
d) Государственная тайна.

31. Получение доступа к информации субъектом в нарушение действующей политики разграничения доступа называется…
a) Несанкционированный доступ;
b) Злоумышленный доступ
c) Неразрешенный доступ;
d) Запретный доступ.

Согласована на портале № 33456

32. Какой вид информации не относится к категории конфиденциальной информации?
a) Коммерческая тайна;
b) Тайна судопроизводства;
c) Персональные данные;
d) Государственная тайна.

33. Каким термином (согласно законодательству РФ) называется любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу?
a) Конфиденциальная информация;
b) Персональные данные;
c) Информация про личность;
d) Информация с ограниченным доступом.

34. Каналы несанкционированного получения информации сгруппированы в…
a) 3 класса;
b) 4 класса;
c) 7 классов;
d) 9 классов.

35. Набор норм, правил и практических приемов, регулирующих управление, защиту и распространение ценной информации, называется …
a) Моделью безопасности;
b) Методом шифрования;
c) Компьютерной безопасностью;
d) Политикой безопасности.

36. Общая, руководящая установка при организации и обеспечении соответствующего вида деятельности, направленная на то, чтобы наиболее важные цели этой деятельности достигались при наиболее рациональном расходовании имеющихся ресурсов – это …
a) Миссия;
b) Стратегия;
c) Функция;
d) Процесс.

37. Что из перечисленного не является целью проведения аудита безопасности?
a) Анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ресурсов системы;
b) Выработка рекомендаций по внедрению новых и повышению эффективности существующих механизмов безопасности системы;
c) Оценка будущего уровня защищенности системы;
d) Оценка соответствия системы существующим стандартам в области информационной безопасности.

38. Выберите неверное утверждение. Сигнатурный метод выявления атак характеризуется:
a) Сравнением исследуемого объекта с ранее известными образцами-эталонами;
b) Способностью обнаруживать ранее неизвестные атаки;
c) Простотой в настройке и эксплуатации для конечного пользователя системы;
d) Популярностью использования в системах антивирусной защиты.

39. Задачи по резервированию системы защиты делятся на:
a) Теплое и холодное резервирование;
b) Холодное и горячее резервирование;
c) Белое и серое резервирование;
d) Толстое и тонкое резервирование.

Согласована на портале № 33456

40. Модель системы с полным перекрытием характеризуется следующим положением:

a) В автоматизированной системе средствами защиты «перекрыто» большинство каналов утечки;

b) В механизме защиты должно содержаться по крайней мере одно средство для перекрытия любого потенциально возможного канала утечки информации;

c) В системе защиты присутствует только одно средство для перекрытия всех угроз безопасности;

d) Автоматизированная система является системой множественного доступа.

41. Инструментальная комплексность в сфере информационной безопасности подразумевает:

a) Непрерывность осуществления мероприятий по защите информации;

b) Защиту информации от внешних и внутренних угроз;

c) Интеграцию всех видов и направлений ИБ для достижения поставленных целей;

d) Обеспечение требуемого уровня защиты во всех элементах системы обработки информации.

42. Какой документ устанавливает цель, задачи и структуру стандартов по защите информации, объединяющий аспекты стандартизации в данной области и являющийся основополагающим стандартом в области защиты информации:

a) ГОСТ Р 52069.0-2013

b) ФЗ №152 от 27.07.2006

c) Постановление Правительства РФ №119 от 01.11.2012

d) Конституция РФ

43. Деятельность по подтверждению характеристик средств защиты информации требованиям государственных стандартов или иных нормативных документов по защите информации, утвержденных Государственной технической комиссией при Президенте Российской Федерации (Гостехкомиссией России) называется

a) Аттестация средств защиты информации

b) Сертификация средств защиты информации

c) Комплексное тестирование средств защиты информации

d) Выборка средств защиты информации

44. Положения Федерального закона №149 от 27.06.2006 не распространяются на:

a) Отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации;

b) Отношения, возникающие при применении информационных технологий;

c) Отношения, возникающие при обеспечении защиты информации

d) Отношения, возникающие при правовой охране результатов интеллектуальной деятельности и приравненных к ним средств индивидуализации

14.1.2. Темы индивидуальных заданий

Выбрать объект защиты из нижеприведенного списка

Для выбранного объекта провести анализ защищенности.

Для выбранного в рамках предыдущего задания объекта провести разработку (усовершенствование) системы защиты.

14.1.3. Зачёт

1. Основные регуляторы
2. Основные нормативно-правовые акты
3. Определения: информация, безопасность информации, защита информации, информационная безопасность, информационный процесс, документ, носитель
4. Свойства информации

Согласована на портале № 33456

5. Виды информации и их определения
6. Государственная тайна
7. Определения: угрозы, несанкционированный доступ.
8. Формы представления информации
9. Классификация угроз
10. Способы реализации угроз
11. Определения: защищаемая информация, доступ, допуск, уязвимость, сзи...
12. Виды защиты информации
13. Конституционные основы в информационной сфере
14. Доктрина ИБ РФ (составляющие национальных интересов РФ)
15. ФЗ «Об информации, информационных технологиях и о защите информации»
16. Преступления в информационной сфере (УК)
17. Задачи организационного обеспечения ЗИ
18. Управление ИБ
19. Модель угроз и модель нарушителя
20. Сложности в работе с персоналом
21. Классификация инсайдерских угроз
22. Социальная инженерия
23. Определения (программно-аппаратная ЗИ): СВТ, доступ, допуск, идентификация, аутентификация
24. Дискреционное и мандатное управление доступом
25. Сертификация
26. Группы классов защищенности АС от НСД
27. Межсетевой экран, антивирус, СОВ
28. Криптографическое преобразование, зашифрование, расшифрование.
29. Хэш-функция и ее свойства
30. Электронная подпись

14.1.4. Темы контрольных работ

1. Основные понятия информационной безопасности. Организационно-правовое обеспечение информационной безопасности.
2. Оценка рисков. Программно-аппаратные средства защиты информации.
3. Политика безопасности. Менеджмент информационной безопасности.

14.1.5. Темы лабораторных работ

Защита персональных данных и коммерческой тайны
Политика безопасности и инструкции для сотрудников предприятия
Оценка рисков информационной безопасности
Защита компьютерной информации на уровне доступа в систему
Защита от атак по локальным и глобальным сетям
Защита от вредоносного ПО
Использование шифрования для защиты данных
Использование физических носителей и защитных систем на их основе
Разработка системы защиты предприятия

14.2. Требования к оценочным материалам для лиц с ограниченными возможностями здоровья и инвалидов

Для лиц с ограниченными возможностями здоровья и инвалидов предусмотрены дополнительные оценочные материалы, перечень которых указан в таблице 14.

Таблица 14 – Дополнительные материалы оценивания для лиц с ограниченными возможностями здоровья и инвалидов

Категории обучающихся	Виды дополнительных оценочных материалов	Формы контроля и оценки результатов обучения
С нарушениями слуха	Тесты, письменные самостоятельные работы, вопросы к зачету,	Преимущественно письменная проверка

Согласована на портале № 33456

	контрольные работы	
С нарушениями зрения	Собеседование по вопросам к зачету, опрос по терминам	Преимущественно устная проверка (индивидуально)
С нарушениями опорно-двигательного аппарата	Решение дистанционных тестов, контрольные работы, письменные самостоятельные работы, вопросы к зачету	Преимущественно дистанционными методами
С ограничениями по общемедицинским показаниям	Тесты, письменные самостоятельные работы, вопросы к зачету, контрольные работы, устные ответы	Преимущественно проверка методами исходя из состояния обучающегося на момент проверки

14.3. Методические рекомендации по оценочным материалам для лиц с ограниченными возможностями здоровья и инвалидов

Для лиц с ограниченными возможностями здоровья и инвалидов предусматривается доступная форма предоставления заданий оценочных средств, а именно:

- в печатной форме;
- в печатной форме с увеличенным шрифтом;
- в форме электронного документа;
- методом чтения ассистентом задания вслух;
- предоставление задания с использованием сурдоперевода.

Лицам с ограниченными возможностями здоровья и инвалидам увеличивается время на подготовку ответов на контрольные вопросы. Для таких обучающихся предусматривается доступная форма предоставления ответов на задания, а именно:

- письменно на бумаге;
- набор ответов на компьютере;
- набор ответов с использованием услуг ассистента;
- представление ответов устно.

Процедура оценивания результатов обучения лиц с ограниченными возможностями здоровья и инвалидов по дисциплине предусматривает предоставление информации в формах, адаптированных к ограничениям их здоровья и восприятия информации:

Для лиц с нарушениями зрения:

- в форме электронного документа;
- в печатной форме увеличенным шрифтом.

Для лиц с нарушениями слуха:

- в форме электронного документа;
- в печатной форме.

Для лиц с нарушениями опорно-двигательного аппарата:

- в форме электронного документа;
- в печатной форме.

При необходимости для лиц с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения может проводиться в несколько этапов.

Согласована на портале № 33456